

SC-300: Microsoft Identity and Access Administrator – Course Plan

Course Overview

This 40-hour course prepares learners for the SC-300 certification. It focuses on managing identity and access using Microsoft Entra ID (Azure AD), implementing authentication, authorization, identity governance, and security best practices as per Microsoft Learn.

Target Audience

- Identity & Access Administrators
- Security Administrators
- System Administrators
- IT Professionals preparing for SC-300

Course Duration

Total Duration: 40 Hours (10 Days | 4 Hours per Day)

Module 1: Identity Concepts & Microsoft Entra ID (4 Hours)

- Identity fundamentals
- Authentication vs Authorization
- Cloud vs Hybrid identity
- Microsoft Entra ID overview
- Tenants, subscriptions, and users

Module 2: User & Group Management (4 Hours)

- Create and manage users
- Groups and administrative units
- Role assignments
- Licensing management
- Guest users and B2B collaboration

Module 3: Authentication Methods & Security (4 Hours)

- Password-based authentication
- Passwordless authentication
- Multi-Factor Authentication (MFA)
- Authentication strength
- Self-service password reset (SSPR)

Module 4: Conditional Access (4 Hours)

- Conditional Access overview
- Policy components
- Risk-based access
- Named locations
- Common CA scenarios

Module 5: Identity Protection (4 Hours)

- Microsoft Entra ID Protection
- User risk & sign-in risk
- Risk policies
- Remediation actions
- Monitoring and reporting

Module 6: Application Management (4 Hours)

- Enterprise applications
- App registrations
- OAuth & OpenID Connect basics
- Permissions & consent
- App proxy

Module 7: Access Management & Authorization (4 Hours)

- Role-Based Access Control (RBAC)
- Privileged Identity Management (PIM)
- Access reviews
- Just-In-Time access

Module 8: Identity Governance (4 Hours)

- Entitlement management
- Access packages
- Lifecycle workflows
- Compliance & audit

Module 9: Hybrid Identity & External Identities (4 Hours)

- Azure AD Connect
- Hybrid identity models
- External identities (B2B/B2C)
- Cross-tenant access

Module 10: Monitoring, Troubleshooting & Exam Prep (4 Hours)

- Logs & monitoring
- Troubleshooting sign-in issues
- Security best practices

- SC-300 exam structure
- Mock questions & revision

Hands-on Labs

- User & group management labs
- MFA & Conditional Access configuration
- PIM & Identity Governance labs
- Application integration demos

Certification Details

Exam Code: SC-300

Duration: 120 minutes

Question Types: Case studies & MCQs

Outcome

After completing this course, learners will be able to design, implement, manage, and monitor identity and access solutions using Microsoft Entra ID.